

0001/2025

I

El proyecto de Orden Ministerial establece diversas medidas para evitar que progresen las comunicaciones con manipulación del identificador de llamada —CLI, por sus siglas en inglés—, introduciendo mecanismos para evitar fraudes en el ámbito de la numeración y los códigos alfanuméricos identificativos de mensajes cortos, y estableciendo medidas para garantizar la correcta identificación de la numeración utilizada para la prestación del servicio de atención a clientes o para la realización de llamadas comerciales no solicitadas.

Según se expone en la MAIN que se acompaña al proyecto de Orden, la norma persigue la defensa de los intereses de los usuarios, proclamada en el artículo 3, letra k), de la Ley 11/2022, de 28 de junio, General de Telecomunicaciones —LGTel—, así como la debida garantía de los derechos de los usuarios establecidos en el artículo 66.1.b) de dicha norma. En atención a este objetivo, se propone el desarrollo de diversas previsiones contenidas, entre otras normas, (i) en el Real Decreto 381/2015, de 14 de mayo, por el que se establecen medidas contra el tráfico no permitido y el tráfico irregular con fines fraudulentos en comunicaciones electrónicas, (ii) en el Real Decreto 424/2005, de 15 de abril (por el que se aprueba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios), y (iii) en el Real Decreto 2296/2004, de 10 de diciembre (por el que se aprueba el Reglamento sobre mercados de comunicaciones electrónicas, acceso a las redes y numeración).

El texto que se informa consta de una parte expositiva, cuatro capítulos con diez artículos, una disposición adicional y tres disposiciones finales.

Tras definir en el artículo 1 el objeto de la norma, centrado en evitar fraudes y garantizar la identificación de numeraciones en el ámbito de las comunicaciones electrónicas, el artículo 2 delimita su ámbito de aplicación, señalando como sujetos obligados a operadores y prestadores de servicios que utilicen numeraciones nacionales o alias. El artículo 3 recoge las definiciones necesarias para interpretar correctamente los términos de la Orden. A continuación, su artículo 4 regula el bloqueo de llamadas con numeraciones vacías, manipuladas o no asignadas, mientras que el artículo 5 se ocupa específicamente del bloqueo de llamadas internacionales que simulen numeraciones nacionales, con ciertas excepciones justificadas. El artículo 6

establece el bloqueo de mensajes SMS, MMS y RCS con numeraciones vacías o no asignadas, y el artículo 7 amplía esta regulación al bloqueo de mensajes internacionales con alias o numeraciones nacionales. Por su parte, el artículo 8 crea un registro obligatorio de alias gestionado por la CNMC, y el artículo 9 prohíbe el uso de numeración móvil para llamadas comerciales y servicios de atención al cliente. Finalmente, el artículo 10 regula el uso de numeraciones de los rangos 800 y 900 para garantizar la gratuidad de las devoluciones de llamadas.

II

*Una primera consecuencia que se extrae del análisis del articulado de la Orden, es que esta **no se enmarca en el ámbito policial o judicial**, regulado por la Directiva (UE) 2016/680, de 27 de abril, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos, y por la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales.*

Es decir, no obstante la denominación de la Orden y las medidas en ella contenidas —dirigidas a combatir las estafas de suplantación y determinadas conductas fraudulentas—, **no se contempla la realización de tratamientos de los previstos en el artículo 1 de la citada Ley Orgánica 7/2021**, de 26 de mayo, cuando dispone que *“tiene por objeto establecer las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos de carácter personal por parte de las autoridades competentes, con fines de prevención, detección, investigación y enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y prevención frente a las amenazas contra la seguridad pública”*.

En segundo lugar, debe tenerse en cuenta que el artículo 4.1 del RGPD define los datos personales como *“toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona”*.

De acuerdo con el contenido del punto 2 del propio artículo 4 del RGPD, se define tratamiento como *“cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización,*

estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción". Por su parte, la definición de "fichero" se contiene en el apartado 6 del artículo 4, que se refiere a "todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica".

El apartado 1 del artículo 2 de la LOPDGDD establece que: "Lo dispuesto en los Títulos I a IX y en los artículos 89 a 94 de la presente ley orgánica se aplica a cualquier tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero."

En este contexto, el Proyecto de Orden contempla diversas finalidades que justifican el tratamiento de datos de carácter personal:

- Bloqueo de comunicaciones fraudulentas: Identificación y bloqueo de llamadas y mensajes de texto que empleen identificadores de llamada (CLI) manipulados o vacíos, así como mensajes SMS/MMS/RCS que no cumplan con los requisitos legales de registro y asignación de numeración.
- Prevención de fraudes: Implementación de medidas para evitar que las comunicaciones con origen internacional simulen identificadores nacionales, con especial atención a los casos de itinerancia internacional.
- Registro y supervisión: Creación de un registro de alias y control de las entidades habilitadas para el envío de mensajes mediante dichos identificadores.
- Garantía de derechos de los usuarios: Establecimiento de medidas que aseguren la correcta identificación de la numeración utilizada en servicios de atención al cliente y llamadas comerciales, para prevenir posibles abusos y garantizar la gratuidad de las devoluciones de llamadas en los rangos 800 y 900.

III

Debe recordarse que la normativa de protección de datos contempla diferentes *bases jurídicas de legitimación* que pueden dar lugar al tratamiento de datos de carácter personal. De acuerdo con el artículo 6 –"Licitud del tratamiento"–, del Reglamento General de Protección de Datos -RGPD-, dicho tratamiento es lícito, y, por tanto, legítimo cuando:

“1. El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:

a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;

b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;

c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento; (la negrita es nuestra)

d) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física;

e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento; (la negrita es nuestra)

f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.

Lo dispuesto en la letra f) del párrafo primero no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones.”

Por su parte, el artículo 8 de la LOPDGDD, que lleva por rúbrica “Tratamiento de datos por obligación legal, interés público o ejercicio de poderes públicos”, en su apartado 2, dispone que:

“2. El tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, en los términos previstos en el artículo 6.1 e) del Reglamento (UE) 2016/679, cuando derive de una competencia atribuida por una norma con rango de ley.”

En este sentido, los tratamientos de datos personales derivados de lo dispuesto en **los artículos 3, letra k**, que persigue la defensa de los intereses de los usuarios, **y 66.1.b)**, que obliga a garantizar la protección de los usuarios frente a prácticas fraudulentas, de la Ley 11/2022, de 28 de junio, General de Telecomunicaciones, encuentran su base de legitimación en el cumplimiento de **una obligación legal aplicable al responsable del tratamiento**, conforme a lo dispuesto en el artículo 6.1.c) del Reglamento General de Protección de Datos (RGPD):

“Artículo 6.1.c):

El tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento.”

A su vez, la implementación del conjunto de medidas previstas en la Orden que se informa, también se ampara, en lo que respecta a la perspectiva de la normativa de protección de datos personales en el interés público reconocido en el artículo 6.1.e) del RGPD, dictándose en virtud de la **competencia exclusiva del Estado en materia de telecomunicaciones**, reconocida en el artículo 149.1. 21.^a de la Constitución.

“Artículo 6.1.e):

El tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.”

IV

Esta Agencia Española de Protección de Datos, en su Circular 1/2023, de 26 de junio, sobre la aplicación del artículo 66.1.b) de la Ley 11/2022, de 28 de junio, General de Telecomunicaciones (BOE 28/06/2023), establece criterios claros para aplicar el citado artículo, que regula el derecho de los usuarios a no recibir llamadas comerciales no deseadas. Este derecho puede ser limitado por el consentimiento previo del usuario o por otras bases de legitimación establecidas en el artículo 6.1 del RGPD. Entre estas bases, además del consentimiento, se incluye el interés legítimo del responsable, siempre que no prevalezcan los derechos y libertades del interesado. La Circular también pretende poner fin a las prácticas de generación aleatoria de números telefónicos para fines comerciales, y establece requisitos específicos para el uso de números en guías de abonados.

En cuanto a los casos en los que las llamadas no se consideran spam, se permite su realización bajo las siguientes condiciones: (i) Consentimiento expreso del usuario para recibir llamadas comerciales, (ii) Interés legítimo, cuando existe una relación contractual previa y los datos fueron obtenidos lícitamente, limitándose a ofertas de productos o servicios similares, y (iii) Tratamiento de los datos de contacto de empresarios individuales o profesionales liberales, en casos relacionados con su actividad profesional, siempre que no se trate de una relación personal.

En todos los supuestos, se requiere cumplir con obligaciones de transparencia, informar sobre los derechos de oposición, consultar sistemas de exclusión publicitaria, y grabar las llamadas para garantizar el cumplimiento normativo.

A su vez, existen diversas normas jurídicas, a las que se ha hecho mención en el **Punto I** de este informe, en las que se establecen (i) medidas contra el tráfico no permitido y el tráfico irregular con fines fraudulentos en comunicaciones electrónicas, (ii) se disponen las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios, y (iii) se aprueban las reglas de funcionamiento de los mercados de comunicaciones electrónicas, acceso a las redes y numeración.

Sin embargo, según se señala tanto en el MAIN del proyecto de Orden que se informa, como en su parte expositiva:

“En los últimos años estamos asistiendo a un incremento exponencial de la cibercriminalidad y, en particular, de las estafas de suplantación de identidad que suelen comenzar con una llamada o un mensaje de texto en los que el emisor de la comunicación suplanta la identidad de una organización de confianza (entidad bancaria, administración pública, empresa de transporte, etc.) con la clara intención de defraudar, engañando al consumidor para que proporcione información personal y financiera confidencial, facilite sus claves personales o realice alguna acción como el acceso a una web, la llamada a un número telefónico, la realización de una transferencia, o la contratación de un servicio, entre otros.

La confianza de los consumidores en la fiabilidad y seguridad del contenido transmitido a través de las redes, el amplio uso que hacen las empresas y organismos de las comunicaciones electrónicas como medio para contactar con sus usuarios, así como la capacidad de estas comunicaciones para llegar a un gran número de personas a un coste relativamente bajo, hacen que el uso de llamadas y mensajes de texto sea un instrumento frecuentemente utilizado en la comisión de este tipo de estafas”.

En consecuencia, el proyecto de Orden Ministerial incorpora una serie de medidas para prevenir la manipulación del número de identificación de llamadas (CLI), evitar fraudes en numeración y alias de mensajería (SMS/MMS/RCS), y garantizar la correcta identificación de números en servicios de atención al cliente y llamadas comerciales no solicitadas.

En el artículo 2 de la Orden, “Ámbito de aplicación”, se contiene la referencia a los responsables de los tratamientos de datos de que se trata, al disponer que:

“1. Las obligaciones establecidas en los Capítulos II y III de la presente orden se aplican a los operadores que presten servicios de comunicaciones interpersonales, los prestadores de almacenamiento y reenvío de mensajes y sus respectivos revendedores en la medida en que permitan establecer comunicaciones (llamadas y mensajes) mediante el empleo de números del Plan Nacional de Numeración Telefónica o de la Orden ITC/308/2008, de 31 de enero, o alias.

2. Las obligaciones establecidas en el Capítulo IV de la presente orden se aplican a los prestadores de servicios de atención al cliente o a quienes realizan llamadas comerciales no solicitadas”.

En su virtud, debe concluirse que dichos **operadores y prestadores de servicio**, actuarán a título de **“responsables del tratamiento”**, en su calidad de *“persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros —ex artículo 4.7 RGPD—*”, siempre, claro está, que existan datos personales que sean tratados, lo que a su vez implica que los interesados a quienes se refieren dichos datos personales sean personas físicas (art. 4.1 RGPD).

V

El artículo 8 del borrador de la Orden, se refiere al registro de alias gestionado por la Comisión Nacional de los Mercados y la Competencia (CNMC). Dicho registro se encuentra diseñado para incluir (i) los alias registrados, es decir, los identificadores utilizados por empresas, administraciones y proveedores de servicios de mensajería para la transmisión de mensajes, y (ii) la identificación de proveedores habilitados, esto es, los datos necesarios para vincular un alias con el proveedor autorizado para su utilización. A saber:

“Artículo 8. Registro de alias y bloqueo de SMS/MMS/RCS con alias no registrados o emitidos por entidades no habilitadas.

1. Las empresas y administraciones que utilicen alias, o los proveedores de servicios de mensajería actuando en su nombre, deberán inscribir dicho alias, con carácter previo a su utilización, en el correspondiente registro gestionado por la Comisión Nacional de los Mercados y la Competencia.

2. El registro contendrá junto con el alias, la identificación de aquellos proveedores de servicios de mensajería habilitados para el envío y transmisión de SMS/MMS/RCS utilizando como identificador el alias inscrito.

3. Los proveedores de redes y servicios involucrados en la transmisión de servicios de mensajería SMS/MMS/RCS deberán bloquear aquellos mensajes SMS/MMS/RCS identificados mediante alias que no hayan sido inscritos en el registro, o que habiendo sido inscritos no hayan sido recibidos de proveedores habilitados en dicho Registro para su envío o transmisión.

4. La Comisión Nacional de los Mercados y la Competencia dictará instrucciones sobre los sujetos obligados, el procedimiento, los requisitos y plazos del proceso de inscripción.”

En consecuencia, del citado artículo 8 de la Orden, parece desprenderse que el mantenimiento de bases de datos gestionadas por la Comisión Nacional de los Mercados y la Competencia (CNMC) para verificar la asignación de numeraciones, se refiere a un **registro de empresas, administraciones y/o proveedores, y no de personas físicas identificadas o identificables**.

Esto es, el precepto transcrito no menciona explícitamente la inscripción de datos personales en el sentido de la normativa de protección de datos (artículo 4.1 del RGPD). A primera vista, parece que este registro se enfoca en los alias y datos técnicos o corporativos relacionados con empresas, administraciones y proveedores habilitados, -en definitiva, personas jurídicas- lo que sugiere que el registro está orientado a la gestión operativa y técnica de las comunicaciones electrónicas, sin implicar la recopilación directa de información que permita identificar a personas físicas, como nombres, apellidos, direcciones o datos de contacto personales.

Sin embargo, aunque el artículo 8 del proyecto no lo especifica, resulta cuando menos teóricamente posible que indirectamente se gestionen datos personales, dependiendo de diversos factores, como la posible existencia de alias relacionados con personas físicas, proveedores individuales y/o representantes legales.

En definitiva, si bien la naturaleza del registro parece centrarse en datos técnicos y corporativos (alias de empresas y administraciones), dependiendo de cómo se implemente su funcionamiento, podría incluir -dado que no se excluye expresamente- datos personales relacionados con personas físicas o representantes legales.

Finalmente, en caso de que se produzcan, a raíz de esa indefinición mencionada, tratamientos de datos personales, se sugiere la incorporación de un nuevo artículo al proyecto de orden, o bien de una disposición adicional, en la que se haga constar la existencia de los tratamientos de datos a los que se refieren los párrafos anteriores, introduciendo un texto que podría ser del siguiente tenor:

“Todos los tratamientos de datos de carácter personal derivados de la aplicación de esta Orden Ministerial, se realizarán con estricta sujeción a lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales, y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, y en la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales, garantizando el derecho fundamental de los afectados a la protección de sus datos de carácter personal”.